



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Business Intelligence Software (QlikView)

US Army Medical Command - DHP Funded System

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System
- New Electronic Collection
- Existing DoD Information System
- Existing Electronic Collection
- Significantly Modified DoD Information System

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR Enter DITPR System Identification Number
- Yes, SIPRNET Enter SIPRNET Identification Number
- No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes
- No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- Yes
- No

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office

Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

Yes

Enter OMB Control Number

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 1071-1085, Medical and Dental Care; 50 U.S.C. Supplement IV, Appendix 454, as amended, Persons liable for training and service; 42 U.S.C. Chapter 117, Sections 11131-11152, Reporting of Information; 10 U.S.C. 1097a and 1097b TRICARE Prime and TRICARE Program; 10 U.S.C. 1079, Contracts for Medical Care for Spouses and Children; 10 U.S.C. 1079a, CHAMPUS; 10 U.S.C. 1086, Contracts for Health Benefits for Certain Members, Former Members, and Their Dependents; E.O. 9397 (SSN); DoD Instruction 6015.23, Delivery of Healthcare at Military Treatment Facilities (MTFs); DoD Directive 6040.37, Confidentiality of Medical Quality Assurance (QA) Records; DoD 6010.8-R, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); Army Regulation 40-66, Medical Record Administration and Health Care Documentation.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

With QlikView, organizations can rapidly deploy fast, flexible Business Discovery apps that provide information workers with dynamic views of the information they need to make decisions. Unlike most business intelligence software, with QlikView information workers can ask and answer the next question, and the question after that, without going back to an expert for a new report or data visualization. The answers are already there, available through simple clicks and taps. At the core of QlikView is our patented software engine, which generates new views of data on the fly. QlikView compresses data and holds it in memory, where it is available for immediate exploration by multiple users. For datasets too large to fit in memory, QlikView connects directly to the data source. QlikView delivers an associative experience across all the data used for analysis, regardless of where it is stored. Users can start anywhere and go anywhere; they are not limited to pre-defined drill paths and preconfigured dashboards. With QlikView's patented core technology, associative experience, and collaboration and mobile capabilities, users can ask and answer streams of questions on their own or in teams and groups, wherever they happen to be working. The more users, the more questions, the more value. Empowering the information workforce to derive insights from data helps organizations streamline, simplify, and optimize decision making. This information will be used to make informed decisions on business processes and assess the efficiencies.

The type of personal information collected is the patient's name, social security number, gender, date of birth, marital status and medical information.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Risks include unauthorized access to PII, inaccurate information in the system, and unauthorized disclosure of PII. There are security measures in place to mitigate these privacy risks. The name of the contractor that will have access to this data is: Qlik Technologies. These security measures are addressed in Section 3d below.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

Within the DoD Component.

Specify.

The PII will be shared with the US Army Medical Treatment Facilities using this application.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

- Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Verbiage from Performance Work Statement, paragraph 10: "SECURITY CLEARANCES/PROTECTION OF SENSITIVE DATA. Security clearances are required. The contractor Qlik Technologies shall follow and comply with all applicable security regulations and policies and shall implement required security measures into final product. They shall maintain confidentiality with regard to all patient-sensitive and business-sensitive information that contract personnel may come in contact with while performing clinical automated systems installation, integration, implementation, sustenance or maintenance."

- Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

- Yes** **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

The patient does not participate in the PII collection process for this application. The PII/ PHI is pulled electronically from multiple sources systems to include: Composite Health Care System (CHCS), Armed Forces Health Longitudinal Technology Application (AHLTA), Clinical Data Repository (CDR), Tactical Operations Center (TOC), ESSENTRIS Electronic Medical Record, Military Health System Mart (M2), Medical System Inventory Repository (MSIR), Joint Medical Asset Repository (JMAR).

j. Do individuals have the opportunity to consent to the specific uses of their PII?

- Yes** **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

The patient does not participate in the PII collection process for this application. The PII/ PHI is pulled electronically from multiple sources systems to include: Composite Health Care System (CHCS), Armed Forces Health Longitudinal Technology Application (AHLTA), Clinical Data Repository (CDR), Tactical Operations Center (TOC), ESSENTRIS Electronic Medical Record, Military Health System Mart (M2), Medical System Inventory Repository (MSIR), Joint Medical Asset Repository (JMAR).

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- Privacy Act Statement
- Privacy Advisory
- Other
- None

Describe each applicable format.

The patient does not participate in the PII collection process for this application. The PII/ PHI is pulled electronically from multiple sources systems to include: Composite Health Care System (CHCS), Armed Forces Health Longitudinal Technology Application (AHLTA), Clinical Data Repository (CDR), Tactical Operations Center (TOC), ESSENTRIS Electronic Medical Record, Military Health System Mart (M2), Medical System Inventory Repository (MSIR), Joint Medical Asset Repository (JMAR).